REMARKS

The Examiner is respectfully requested to reconsider the rejection of claims 7, 9 - 13, 40 and 59 under 35 U.S.C. § 103 (a) as being unpatentable over Cashman, et al. (U.S. Patent 6,209,087) in view of Lincke (U.S. Patent 6,397,259).

The present invention relates to secure proxying for computing devices. The invention is directed toward network security protocols which are used to insure privacy and integrity of communication on an open public network. These protocols are intended to achieve end-to-end security guarantees such that the communication is private to the entities that establish the parameters of the secure communication channel. Applicants emphasize that "Security guarantee" is an essential feature of the invention.

Claim 7 defines the use of a secure coprocessor which is used to achieve end to end security guarantees in the protocol translation between client and server. This feature assures that the proxy cannot tamper with the functioning of the agent and view unencrypted communication between said client and said server. The agent is a software program or hardware logic operating within the confines of the secure coprocessor.

Cashman et al., as discussed later in greater detail, describe a method which uses a coprocessor to implement elements of the protocol translation process between client and server. The Examiner does not accept that the coprocessor (which is under the control of the proxy) is trusted differently from the secure coprocessor in Applicants' claim which secure coprocessor enforces a very strong trust model. Claim 7 states that the protocols that the secure coprocessor will splice are the security protocols of WAP and SSL/TLS. The Examiner has acknowledged that this "splice" feature is not found in Cashman. In Cashman's system, the proxy is trusted to do the aforementioned protocol translation, and the coprocessor is used merely as performance-enhancing means. It is submitted respectfully that the Examiner is not interpreting the teaching of the Cashman reference correctly.

Note that in Cashman, the proxy can, and does tamper with what the coprocessor does. In Cashman, the proxy directly controls the coprocessor. Applicants re-emphasize that there is no end to end security guarantee being maintained by the protocol translation process of Cashman as is the case in the present invention. The Cashman protocol translation process is different from that claimed by Applicants.

The unique feature of Applicants' invention is the trust model of the splicing. In Applicants' invention the secure coprocessor does not trust the server, whereas in Cashman, the CPU is an integral portion of the protocol translation. Note that in Cashman's scheme, the contents are available unencrypted to any agent/process on the proxy. This is an important feture to be considered.

A key word in the present invention is "trust." In Applicants' invention, the coprocessor and the proxy do NOT trust each other. This concept is detailed in Claim 7, which *inter alia* states: "embedding a secure coprocessor for use as an agent of said client and/or said server which assures that said proxy cannot tamper with the functioning of said agent and view unencrypted communication between said client and said server, said agent being a software program or hardware logic operating within the confines of said secure coprocessor..." The Examiner contends that the excerpt cited above is taught in Cashman at "fig.1, see col.7, lines 48-65." Applicants respectfully submit that the teaching at the location cited (or anywhere in Cashman) does not teach the trust aspect as between coprocessor and proxy as Applicants have claimed in the excerpt. There is a distinct difference between what Applicants claim and what Cashman teaches. In Column 8, lines 5 - 8, Cashman says the CPU instructs the coprocessor to concurrently encrypt and compress and packetize data which is does and then notifies the CPU. This teaching of encrypting and compressing is no basis for properly asserting that Cashman meets the language excerpted above as to the role of the proxy as claimed. Cashman's words do not say what the Examiner says they do. The simple act of encryption and compression does not meet the function of the proxy. In reviewing the overall Cashman system, there is not the security (trust) feature in place as among the entities present which is claimed by Applicants.

Cashman does not disclose each and every element defined in Applicants' Claim 7, et al. The Examiner thus cites Lincke, et al. to supplement the Cashman reference to supply the specific teaching that she asserts Cashman is lacking. Succinctly stated, the Lincke invention is focused on transcoding for wireless devices and optimizing the communication from the proxy to the client.

Lincke discloses an improved system and method for using a handheld device to access Internet information over relative low bandwidth networks. Lincke is directed toward a communications system which includes the wireless communications device, a server, and a source of data. The server acts as a proxy server. Typical sources of data are a web server or a mail server. In reviewing the Lincke, et al. patent, as noted below, the disclosure does not address the issue of splicing a plurality of secure communication protocols which is a security protocol of a WAP to that of an IP device. Essentially, Lincke seeks to optimize the number of messages sent to a wireless client.

The objective Lincke, et al. sought to emphasize was to consider wireless networks, such as two-way pagers and other wireless packet data networks, which provide wider coverage and lower cost than competing networks. These wireless networks typically have relatively low performance however. A single packet of 400 bytes can take eight seconds just to travel to the Internet and back when the system is lightly loaded. With such a low throughput, it could easily take minutes to download even a small web page using standard browser technology. The wireless communications system therefore employs novel methods for reducing the amount of traffic sent over the wireless link for web access. The skilled artisan would consider these deficiencies when reflecting on wireless communication systems.

Lincke, et al. wanted to provide the user with fast access to web content. Although the wireless communications device can access generic web content, because of the wireless communications device's limited screen size, most existing content will not be as visually appealing, will be harder to navigate, and may take longer to access than specially formatted content. Thus, significant advantages are achieved with customized content. The web content can

be formatted for the small screens of most handheld communications devices. This content will download relatively quickly (because of its small size). The formatted content can be created and published using the same tools used today for desktop web publishing (i.e. HTML tools and web servers) and could even be viewed using a standard desktop browser.

Applicants use the coprocessor in their invention to enforce a trust model between the client and the server. The secure coprocessor guarantees that no external entity can tamper with the functioning of the hardware logic or software programs. The use of the coprocessor in the present invention insures that end to end security is guaranteed. Again something that Cashman does not insure nor does Lincke even consider.

It is essential to note in the present invention, neither the proxy nor any external entity can tamper with the functionality being implemented by the software programs or hardware logic functioning with the confines of the coprocessor. This is not found in Lincke, et al.

Applicants respectfully submit that the specificity of the Cashman and Lincke disclosures alone or in combination, do not directly disclose or even imply the method of providing secure communication of the present invention as presently claimed. In the rejection, the Examiner is picking and choosing elements to the exclusion of what the references as a whole teach to one skilled in the art.

In order to analyze the propriety of the Examiner's obviousness rejections in this case, a review of the pertinent applicable law relating to 35 U.S.C. § 103 is warranted. The Examiner has applied the Cashman and Lincke, et al. references using selective combinations to render obvious the invention.

Cashman at Column 1, lines 29 - 39 discloses that "During data communications, the manner in which bits of data are specifically arranged and the order in which they are exchanged between devices is called a protocol...There are many different types of protocols serving different purposes, but each typically involves a sending device that arranges data in one manner, and a receiving device that detects the specific arrangement of the data in order to make use of the data upon reception."

Cashman then discloses that the CPU is responsible for performing protocols on data and exemplifies the activities so performed. (Column 1, lines 51 - 63). Cashman cites examples of protocols which are in the prior art such as V.42bis, HDLC, SLIP and PPP and CRC. (Column 2, lines 5 - 63).

It is a column 3, lines 1 to 20, that Cashman states that these protocols "...suffer a variety of problems..." It is at Column 3, starting at line 21, etc. that Cashman details that his invention overcomes the problems with the prior art. He states that "The present invention provides a network device (with CPU) including a *unique co-processor* having symmetrical architecture and an extended processor instruction set..." See Column 5 for a detailed disclosure of the extension processor instruction logic circuits and specifically the "...XALU created according to this invention." The manner in which the Cashman invention operates is detailed in Columns 5 and 6 of the patent.

Applicants respectfully point out that Columns 5 and 6 of the Cashman disclosure explain all of the many features of the system that make it, in his own words, unique, i.e., *being with out a like or equal.* The disclosure referred to above clearly establishes that there are many very specific features which must be considered when seeking to combine this reference with another. The skilled artisan, in reviewing the reference is going to interpret the teaching as applying to a network device having a CPU, etc., as described in Column 7, lines 48 - 65. The Cashman's unique system is not designed for a wireless application.

In the January 13, 2005 Official Action, the Examiner stated that *"...claims 7, 9 - 13, 40 and 59 are allowable for the features of splicing a plurality of secure communication protocols of different protocol suites into the agent, wherein the step of splicing a plurality of secure communication protocols is a security protocol of a WAP to that of an IP...Cashman does not disclose these protocols..."* The Examiner has conceded therein that Cashman does not disclose those elements. As noted above, the Examiner subsequently cited the Lincke reference applying it in combination with Cashman.

Lincke discloses a wireless communications system. Lincke states in his preliminary remarks that in a high bandwidth network system, such as a wired network, (like Cashman) the

usual techniques for browsing data on the Internet are adequate. (Column 3, lines 2 - 5). At Column 3, lines 6 - 32, Lincke explains how, using a wired CPU, one connects to the Web. He then explains at Column 3, line 33 etc., that "for low bandwidth networks, this *TECHNIQUE DOES NOT WORK WELL.*" (Emphasis added) Even if connected to a high bandwidth network, most handheld devices do not have screen area or processing power to display the graphics and large amounts of text in a typical web page. Further problems with the prior art are found in Column 4, lines 5 - 40. It is clear that Lincke, in his disclosure, seeks to distance his invention from the wired networks and previous wireless systems.

The Lincke system is very specific. It contains specified elements used in the wireless communication system; it has a network topology with very specific protocols (which would not be compatible with the Cashman system) used to communicate among the various devices in the system; it has its own CML markup language, and other features unique to it alone.

The Examiner asserts that the language in Claim 7 "wherein the step of splicing a plurality of secure communication protocols is a security protocol of a Wireless Application Protocol Suite (WAP) to that of an Internet Protocol (IP) device," is disclosed at col.9, lines 56-67, col.10, lines 1-2, col. 11, lines 8-25 of Lincke. Applicants respectfully disagree. There is no such disclosure at the locations cited in Lincke. The disclosure of Lincke at col. 11, lines 8-17 relate to a wireless system. There is no teaching in Lincke which positively equates the wireless system with the wired network systems. In fact, as cited above, Lincke states that they are different.

The Examiner's obviousness rejection of the claims is incomplete as she has not provided the proper evidentiary foundation for the rejection. The predicate for the combination of Lincke with Cashman comes, not from the disclosures found in the text, but rather based upon the assumptions that the Examiner contends would occur in mixing the wired system of Cashman with the wireless system of Lincke. The two specific systems to Cashman and to Lincke are totally different. There is no proper basis to combine them.

The Court of Appeals for the Federal Circuit has set guidelines governing such application of references. These guidelines are, as stated are found in Interconnect Planning Corp. v. Feil, 774 F.2d 1132, 1143, 227 USPQ, 543, 551:

> When prior art references require selective combination by the court to render obvious a subsequent invention, there must be some reason for the combination other than hindsight gleaned from the invention itself.

A representative case relying upon this rule of law is Uniroyal, Inc. v. Rudkin-Wiley Corp., 837 F.2d 1044, 5 USPQ 2d 1434 (Fed. Cir. 1988). The district court in Uniroyal found that a combination of various features from a plurality of prior art references suggested the claimed invention of the patent in suit. The Federal Circuit in its decision found that the district court did not show, however, that there was any teaching or suggestion in any of the references, or in the prior art as a whole, that would lead one with ordinary skill in the art to make the combination. The Federal Circuit opined:

> Something in the prior art as a whole must suggest the desirability, and thus the obviousness, of making the combination. [837 F.2d at 1051, 5 USPQ 2d at 1438, citing Lindemann, 730 F.2d 1452, 221 USPQ 481, 488 (Fed. Cir. 1984).]

With respect to the combination of the Cashman and Lincke, et al. references, the Examiner has selected elements from these references for the sake of showing the individual elements claimed (e.g., protocol, server, proxy, client, agent) without regard to the total teaching of the references. As noted, the Examiner is improperly picking and choosing. The rejections are a piecemeal construction of the invention. Such piecemeal reconstruction of the prior art patents in light of the instant disclosure is contrary to the requirements of 35 U.S.C. § 103.

> The ever present question in cases within the ambit of 35 U.S.C. § 103 is whether the subject matter as a whole would have been obvious to one of ordinary skill in the art following the teachings of the prior art at the time the invention was made. It is impermissible within the framework of Section 103 to pick and choose from any one reference only so much of it as will support a given position, to the exclusion of other parts necessary to the full appreciation of what such reference fairly suggests to one of ordinary skill in the art. (Emphasis in original) In re Wesslau 147 U.S.P.Q. 391, 393 (CCPA 1965)

This holding succinctly summarizes the Examiner's application of references in this case because she did in fact pick and choose so much of the Cashman and Lincke, et al. disclosures to support her position and did not cover completely in the Office Action the full scope of what

these varied disclosure references fairly suggest to one skilled in the art.

As noted above, Lincke, et al. desire to provide the user with fast access to web content. Cashman teaches against Lincke's objective stating at Column 3, lines 6 - 8 that *"A CPU executing a program to compress and encrypt data must process data fast enough to fully utilize available data communications bandwidth. Fast processors are expensive and increase the cost of data communications devices."* Lincke, et al. state that "*A goal of the invention is to provide the user with fast access to web content.*" The goals stated by these teachings are diametrically opposite. There is no basis to combine the references as has been done in the Official Action based upon their respective teachings and objectives. The Examiner has already stated on the record that the Claims are patentable over Cashman. Essentially, the Lincke, et al. disclosure is a non-analogous art based upon its teaching with respect to Cashman.

Further, the Federal Circuit has stated that the Patent Office bears the burden of establishing obviousness, and that this burden can only be satisfied by showing some objective teaching in the prior art or that knowledge generally available to one of ordinary skill in the art would lead that individual to combine the relevant teachings of the reference.

> Obviousness is tested by "what the combined teachings of the references would have suggested to those of ordinary skill in the art." In re Keller, 642 F.2d 413, 425, 208 USPQ 871, 881 (CCPA 1981). But it "cannot be established by combining the teachings of the prior art to produce the claimed invention, absent some teaching or suggestion supporting the combination." ACS Hosp. Sys., 732 F.2d at 1577, 221 USPQ at 933. [837 F.2d at 1075, 5 USPQ 2d at 1599.]

The Court concluded its discussion of this issue by stating that teachings or references can be combined only if there is some suggestion or incentive to do so.

In the present case, the skilled artisan viewing the Cashman and Lincke, et al. references would not be inclined to combine the be directed toward a totally different system than is called for in the present invention. There is no teaching in Lincke, et al. directed toward Applicants' objective of use a secure coprocessor to perform protocol translation in a manner that preserves the end to end trust model between the client and server. There is no mention of security and one

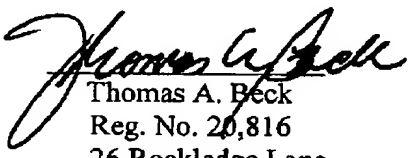
cannot assume that combining the entire teaching of Lincke, et al. with Cashman would not compromise the Cashman system. The skilled artisan must consider the entire teaching of Lincke, et al. before combining it with Cashman. Applicants' Claims define a "secure coprocessor" which explicitly means tamper resistant/ tamper-proof and further means that the coprocessor is translating protocols while still maintaining the trust model between the client and server. Neither Cashman nor Lincke, et al. disclose those elements. The combination is improper.

If there are issues which could be resolved by a telephone conference, Applicants' attorney would be willing to speak with the Examiner concerning such matter(s) at a mutually convenient time. The Examiner is requested to contact Applicant's attorney by telephone at the number listed below.

Applicant has attempted to distinguish the invention as embodied in the amended claims over the prior art. In view of the arguments and modifications to the claims, allowance of this case is warranted. Such favorable action is respectfully solicited.

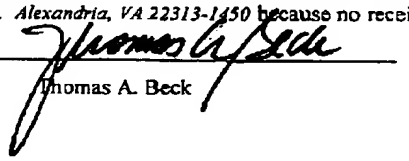
August 4, 2006

Respectfully submitted,



Thomas A. Beck
Reg. No. 20,816
26 Rockledge Lane
New Milford, CT 06776

I certify that this amendment is being re-telefaxed to (571) 273-8300 on the date shown below addressed to: *Assistant Commissioner of Patents, P.O. Box 1450, Alexandria, VA 22313-1450* because no receipt of transmission was received by Applicants' Attorney.

Signature  Date: August 3, 2006

Name: Thomas A. Beck